ABSTRACT OF THE DISCLOSURE

The present invention relates to a method for detecting malicious code patterns in consideration of control and data flows. In the method of the present invention, a malicious code pattern is detected by determining whether values of tokens (variables or constants) included in two sentences to be examined will be identical to each other during execution of the sentences, and the determination on whether the values of the tokens will be identical to each other during the execution is made through classification into four cases: a case where both tokens in two sentences are constants, a case where one of tokens of two sentences is a constant and the other token is a variable, a case where both tokens of two sentences are variables and have the same name and range, and a case where both tokens of two sentences are variables but do not have the same name and range. According to the present invention, it is possible to exclude a false positive error that may occur in conventional comparison of variable names and to lower a false negative error rate, thereby improving the accuracy of detection of malicious behaviors.